REMARKS

Submitted herewith is a petition to extend the time for response from 8 December 2004 to 8 March 2005.

As a result of this amendment, the claims now pending in this application are claims 2, 4 - 7, 11 - 13, 16, and 18 and new claims 20-28.

Claim 1 has been rewritten as new claim 20, and claim 2 formerly dependent on claim 1 has been amended to depend from claim 20.

Claims 1, 3 - 8 and 16 - 19 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite because of use of the words "may", "institution" and "PIN". Applicants respectfully request reconsideration of the rejection since (a) claims 1 and 3 have been canceled and thereby eliminate the objection to "may", (b) the word "institution" has been deleted from the claims, and (c) the objection to "PIN" is not well founded since that term is defined in the specification at page 3, line 6. In any event, certain of the claims that contain that term have been amended to call for a "PIN as herein defined".

Applicants further request reconsideration of the rejection of the original claims under 35 U.S.C. 103(a) as being unpatentable over Nissl et al in view of Pinizzotto. This request is premised on the fact that neither of those references discloses, suggests or renders obvious Applicants' invention and also on the fact that Applicants have amended the claims to patentably distinguish their invention from those references and also the other prior art of record.

The purpose of Applicants' invention is to reduce the risk of credit fraud by allowing a credit card user to acquire a unique encrypted time-limited number that is based on his valid credit card information and may be used in completing a credit card transaction. Essentially that unique number functions as a time-limited credit card number that a third party vendor can

accept for verification by the credit card issuer or a party authorized by the credit card issuer.

As noted on page 1 of the application, in the section labeled "Background of the Invention", the information required to initiate a credit card transaction for the purchase of goods and services consists of a credit card number, an expiration date and the card holder's name and billing address. According to this invention a date/time stamp is embedded into or accompanies the credit card transaction information provided by the user and serves to limit the useful life of that transaction information (see sentence bridging pages 1 and 21 of the application). That date/time stamp is encrypted using a software program supplied by the credit card issuer (see page 2, lines 22-24; page 5, lines 6-10). Some of that required transaction information, e.g., credit card number and user's personal identification code (PIN) is also encrypted (see pages 3, lines 22-25, page 8, lines 8-26) to provide an encrypted time-limited credit card number, e.g., the ePIN described on page 8. That encrypted time-limited credit card number is supplied by the user to a vendor and the vendor in turn transmits that information to the credit card issuer or some other party authorized by the credit card issuer to validate the transaction.

The validation process involves decrypting the time-limited credit card number, e.g., the ePIN, determining the validity of the decrypted information by comparing it to information previously recorded by the credit card issuer or the authorized validating party and also determining whether the time indicated by the decrypted date/time stamp is within a predetermined time limit known to the validating party, and communicating validation or rejection of the proposed credit card transaction to the vendor and/or the party initiating the proposed transaction on the basis of the acceptability of the decrypted time stamp and decrypted credit card information.

A further aspect of the invention is that in its preferred embodiments the user initiates the transaction employing a computer with an internet browser,

with the computer software that generates the unique card number comprising an encrypted date/time stamp being provided by the credit card issuer or a party authorized by the credit card issuer to verify and validate credit card information for proposed transactions. That computer software may be installed on a user's browser-equipped computer or on a remote server controlled by the credit card issuer or the authorized validating party.

The claimed invention offers the advantage of flexibility as well as security. Flexibility is achieved by virtue of the fact that the period of time during which the unique card number will be accepted for a proposed credit card transaction can be varied. That period could be for hours or one or more days or months. Furthermore, the method may be adjusted to allow the credit card user or the credit card issuer to determine the length of time that the unique card number can be used to execute a proposed transaction. Hence if that unique credit card number is stolen from the vendor's database, no loss will ensue unless it is used within its predetermined lifetime.

A further advantage is that software used to generate the unique encrypted time-limited number may be a software applet that is distributed to a credit card holder at the same time as or after the credit card is issued. This software may be installed on an authorized user's palm device or a custom "smart card" device instead of or in addition to being installed on his computer. Still another advantage of the invention is that different banks implementing the method may use distinct and unique encryption methods appropriate to the level of security desired. The nature and source of the software used for encryption is set forth in the application.

A critical and novel aspect of the invention is that in its preferred embodiment the creation of the encrypted credit card occurs using software installed on the card user's computer and does not require interaction with the credit card issuer or any party acting for the credit card issuer. Moreover the unique encrypted time-limited number may be transmitted to the vendor orally via a telephone conversation of in face-to-face meeting with a vendor. In such

case the institution or vendor receiving the encrypted credit card number for a transaction processes it as it would any other credit card transaction.

The claims now in the application all call for the encryption features described above. Those claims are believed to define patentably over Nissl et al. and Pinizzotto, whether considered individually or collectively, for the following reasons.

Nissl et al. U.S. Patent No. 6,530,023 pertains to a specific method for sealing data to protect it against unauthorized access or manipulation (col. 2, lines 56-60). It achieves this by incorporating in the data, during the encryption process, a date/time stamp and an authentication code, e.g., a signature. This encrypted data is then transmitted to a selected receiver. At the receiver end, the encrypted data remains blocked (i.e., sealed) and can be accessed only after it has been decrypted and subjected to manipulation and authentication checks. At the conclusion of these checks, the data file is again in readable form. It appears from column 4, lines 1-11, that in the Nissl et al. method the time and date are required to decrypt the transmitted data and permit access to the sealed data.

In contrast to the Nissl et al. method, Applicants method utilizes a date/time stamp to create a unique encrypted number that includes encrypted credit card information, and when that number is decrypted, the time and date are used to verify that the time for conducting the transaction has not expired. Furthermore, unlike Nissl, Applicants' method includes the unique step of transmitting the results of the validating process to a vendor and/or the person initiating the proposed credit card transaction.

In a preferred embodiment of the invention, the unique encrypted card number comprises not just an encrypted date/time stamp but also encrypted credit card information, e.g., credit card number and/or a PIN. In other words, the credit card information and the date/time stamp form one unique encrypted time-limited card number. This concept is completely foreign to Nissl et al.

Pinizzotto patent application 20030097343 discloses a method that differs from Applicants' in that the vendor does not receive a credit card number. A processing center sits between the user (customer) and the vendor, and that device commits the transaction and provides the vendor with payment validation. The vendor does not have access to the client's credit card number. The customer's credit card information is encrypted at the customer ordering terminal and then sent to the processing center. The user must have internet access to transmit the encrypted request to the processing center and the processing center must have a means of sending the payment validation to the vendor. Other systems using a trusted agent as a transaction intermediary are well known, as exemplified by U.S. Patent No. 5,703,949, issued Dec. 30, 1997 to Sholom S. Rosen for "Method for Establishing Secure Communications Among Processing Devices".

Pinizzotto's and Applicants' method are similar in that the vendor never has access to the customer's credit card number, but the present invention differs and provides additional security and flexibility by virtue of the fact that the information given to the vendor sees a unique encrypted card number that is good for only a limited time, and that unique number is received directly from the customer. As a consequence, the customer can provide the unique number to a vendor orally via phone or in face-to-face dealing for a proposed transaction, and that vendor can confirm that number with the credit card issuer or other authorized validating entity as he would any other credit card number. That is not possible using Pinizzotto's method.

Since the Nissl et al. and Pinizzotto methods differ substantially from one another and also from Applicants' in both purpose and steps, Applicants submit that modifying the Nissl et al. method to incorporate steps or procedures from the Pinizzotto method, or vice versa, is not obvious from either of those references and also would not result in a method corresponding in steps, purpose and advantages to the method defined by Applicant's claims, all of which relate to electronic credit card transactions and call for a time-

limited date/time stamp or a unique number that comprises an encrypted date/time stamp. It should be noted that the new claims submitted herewith differ from the remaining original claims only in scope and are designed to assure proper coverage for the invention. In this connection, claims 30 and 31 are directed specifically to electronic transactions involving a bank and another entity. The method defined by claims 30 and 31 is unique and not anticipated or suggested by Nissl and/or Pinizzotto.

The other references made of record by the Examiner in the Official Action also do not anticipate or render obvious Applicants' claimed invention.

Barkan's U.S. Patent No. 5,864,667 describes a hardware apparatus and method for transferring the encryption key in a secure way to establish a secure communication link. At column 4, line 18, the patent states:

> "According to an eighth aspect of the present invention, the certificate may be used for secure payment over insecure links, for example the Internet. The credit card information is protected from unauthorized use by the seller or third parties participating in Internet for example, by the inclusion of the credit card information in the encrypted certificate, with that certificate capable of being decrypted only by the authorized party, the credit card issuer for example."

In this case the user's credit card information is encrypted based on a private encryption key. The user and the bank both have to know the encryption key to encrypt/decrypt the certificate or credit card number. The security of this patented method must depend on frequently changing the private encryption key. Hence a number encrypted with an earlier key could not be decrypted by the bank once a new encryption key is in place, preventing reuse of the data. The data transmitted to the vendor can be reused until the encryption key is changed.

Barkan's patented method differs from Applicants' in that it does not produce a unique encrypted credit card number that may be used for a credit card transaction so long as that transaction occurs within a predetermined time of a time included in the encrypted card number. In further contrast to

Barkans's method, Applicants' method does not require a user generated encryption key. Applicants' method also has the advantage that more credit card information can be included with the encrypted data than covered by the Barkan patent. Also with Applicants' method the credit card user has no control over the encryption algorithm itself, and is not privy to the encryption key. Although a bank implementing Applicants' method is free to use an encryption system which requires that both the bank and the client know an encryption key, but the encryption and decryption are left entirely to the domain of the bank or other credit card issuer.

Frith et al. U.S. Patent No. 5,943,426 discloses a method that requires attaching a digital signature to a message to authenticate the message. The method involves data reduction and reconstruction of messages that have digital signatures attached. Applicants' method does not involve data compression and reconstruction and does not require a digital signature. Applicants' method does not authenticate the message but instead is used to disguise the customer's credit information and limits the time that the unique card number is valid.

In view of the foregoing remarks and the changes and additions to the claims, it is believed that this amendment places this application in condition for allowance. Therefore, prompt and favorable reconsideration is solicited.

Respectfully submitted,

3/7/05

Nicholas A. Pandiscio
Reg. No. 17,293
Pandiscio & Pandiscio
470 Totten Pond Road
Waltham, MA 02451-1914
Tel. (781) 290-0060
Fax (781) 290-4840

Mailing Certificate

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, sufficient postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner For Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below:

7 MARCH 2005

(date of deposit)

NICHOLAS A. PANDISCIO

(name of attorney)

Nicholas A Pandiscio

(signature)

VASIL-1.AMA revised FINAL 3/7/05